REMARKS

The Examiner has maintained the rejection of the claims. As set forth below, such rejection is still deficient. However, despite such deficiencies and in the spirit of expediting the prosecution of the present application, applicant has incorporated the subject matter of at least one dependent claim into each of the independent claims. Since the subject matter of such dependent claim(s) was already considered by the Examiner, it is asserted that such claim amendments would **not** require new search and/or consideration.

The Examiner has objected to Claims 12, 26, 40 and 54 for reciting an acronym. Applicant has clarified each of the forgoing claims by spelling out the acronym to avoid such objection.

The Examiner has rejected Claims 1-2, 5, 8, 15-16, 19, 22, 29-30, 33, 36, 43-44, 47 and 50 under 35 U.S.C. 102(e) as being anticipated by Hartley et al. (U.S. Patent Application No. 2002/0026591). In addition, the Examiner has rejected Claims 6-7, 9-14, 20-21, 23-28, 34-35, 37-42, 48-49, and 51-56 under 35 U.S.C. 103(a) as being unpatentable over Hartley in view of Jenevein (U.S. Patent No. 6,615,365). Applicant respectfully disagrees with such rejections, especially in view of the amendments made hereinabove to each of the independent claims.

With respect to each of the independent claims, the Examiner has relied on paragraph [0035], as excerpted below, and specifically database 42 in Hartley to make a prior art showing of applicant's claimed "creating a database of the known scanned regions of the verified file system" (see the same or similar, but not necessarily identical language in each of the independent claims).

> "[0035] Disclosed in FIG. 3 is a system diagram for the directory check module 18. The directory check module receives data from two sources. The first being the security system database 30 and the second being file system database 42, which is a listing of files and directories in the system memory including pertinent

> information relating file or directory ownership, group ownership, and times in which any changes were made to the file or directory. Upon completion of the analysis, a report may be issued via report module 29" (emphasis added).

Applicant respectfully asserts that the file system database (item 42) in Hartley is only "a listing of files and directories in the system memory." Clearly, a listing of all files and directories in a system does not meet applicant's claimed "database of the known scanned regions of the verified file system" (emphasis added).

Still with respect to each of the independent claims, the Examiner has relied on the following excerpt from Hartley to make a prior art showing of applicant's claimed "validating an integrity of an object in the file system against the database of known scanned regions" (see the same or similar, but not necessarily identical language in each of the independent claims).

> "[0041] Disclosed in FIG. 5 is a system diagram which includes the data stores accessed by the integrity check module 22. As described above, the integrity check module is employed to analyze the computer system and identify vulnerabilities and discrepancies. Data to be analyzed is retrieved from the file system table of contents 72 which includes a listing of files to be analyzed. Also in connection with the integrity module is the **vulnerability database 70 which includes a listing of potential vulnerabilities. Items contained in the vulnerability database which are employed when analyzing a filed**, may relate to age, owner, permissions, existence and group. Any vulnerabilities or discrepancies detected during the process are output via the report subsystem 29" (emphasis added).

Applicant respectfully asserts that Hartley only discloses a vulnerability database that "includes a listing of potential vulnerabilities" (see emphasized excerpt above). Thus, in Hartley, the data is only analyzed against the database of potential vulnerabilities. Applicant on the other hand, claims "validating an integrity of an object in the file system against the database of known scanned regions" (emphasis added). Clearly, potential vulnerabilities, as in Hartley, do not meet applicant's claimed scanned regions.

Furthermore, the Examiner has relied on paragraphs [0041]-[0043] and [0049] in Hartley to make a prior art showing of applicant's claimed technique "wherein the verifying comprises: receiving a file system event from a real-time monitoring system, the file system event indicating that an object in the file system has been accessed." Applicant respectfully asserts that such excerpts only generally teach that "[d]ata to be analyzed is retrieved" (paragraph [0041]), that "operations of the network interface 14 are analyzed...[such that the] identification of excessive system services may be determined" (paragraph [0043]), and that "[security system] modules [perform] particular functions" (paragraph [0049]).

Clearly, none of such teachings specifically disclose "receiving a file system event from a real-time monitoring system," let alone where such "system event indicat[es] that an object in the file system has been accessed," as claimed by applicant (emphasis added). In particular, merely analyzing operations of a network, as in Hartley, does not meet events that are received from a real-time monitoring system, in the manner claimed by applicant. Furthermore, simply nowhere does Hartley specifically disclose any sort of event "indicating that an object in the file system has been accessed," as applicant claims.

Even still yet, the Examiner has relied on paragraphs [0048] and [0068] in Hartley to make a prior art showing of applicant's claimed "flagging the database of known scanned regions to indicate which of the known scanned regions was occupied by the accessed object; wherein the validating utilizes the flagging." Applicant respectfully asserts that Hartley only teaches "manually mark[ing] a file which may be critical to the computer system...[such that] the file [is] checked by the directory check module each time it is run." Thus, in Hartley, a file is checked, whereas applicant claims "flagging the database of known scanned regions" (emphasis added). Furthermore, in Hartley the file is checked if it is critical to the computer system. Applicant however, claims "flagging... to indicate which of the known scanned regions was occupied by the accessed object" (emphasis added).

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Hartley reference, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has substantially incorporated the subject matter of Claims 5, 6 and 9 et al., at least in part, into each of the independent claims.

With respect to the subject matter of Claim 5 et al., the Examiner has relied on paragraph [0041] in Hartley, as excerpted above, to make a prior art showing of applicant's claimed technique "wherein the database of known scanned regions comprises a copy of a partition table data structure indicating an identity and a location of a known scanned region occupied by the object" (see this or similar, but not necessarily identical language in each of the independent claims). Applicant respectfully asserts that such excerpt only discloses a "listing of files to be analyzed" and a "vulnerability database." Clearly, such list and database in Hartley does not meet applicant's claimed "copy of a partition table data structure," let alone where such partition table data structure indicates "an identity and a location of a known scanned region occupied by the object," as claimed (emphasis added).

With respect to the subject matter of Claim 6 et al., presently incorporated, at least in part, into each of the independent claims, the Examiner has relied on Col. 11, lines 8-15; Col. 13, line 15-Col. 14, line 27; and Col. 15, lines 20-33 in Jenevein to make a prior art showing of applicant's claimed technique "wherein the partition table data structure includes an inode that contains information about the object other than name, and a directory block that contains the object name and a number of the inode of the object"

(see this or similar, but not necessarily identical language in each of the independent claims).

Applicant respectfully asserts that Jenevein only teaches a file ID which identifies which file the block belongs to and a sequential ID which identifies each block's sequence number. Applicant notes that the identifiers in Jenevein do not even relate to a "partition table data structure," as applicant claims, but instead only relate to header information contained in a block (see Col. 11, lines 8-9). Furthermore, neither the file ID nor the sequential ID in Jenevein meet applicant's claimed directory block that contains the object name and "a number of the inode of the object" (emphasis added).

Still yet, with respect to the subject matter of Claim 9 et al., presently incorporated, at least in part, into each of the independent claims, the Examiner has relied on col. 11, lines 8-15; col. 13, line 15 – col. 14, line 27; and col. 15, lines 20-30 in Jenevein to make a prior art showing of applicant's claimed technique "wherein flagging comprises indicating which of the inodes and directory blocks were occupied by the accessed object" (see this or similar, but not necessarily identical language in each of the independent claims). In response, applicant notes that Jenevein fails to even teach any sort of flagging as applicant claims, let alone indicating which inodes/directory blocks are occupied by the accessed object.

Applicant respectfully asserts that the Hartley reference, when taken alone and in combination with Jenevein, fails to teach or even suggest all of applicant's claim limitation, especially in view of the amendments made hereinabove to each of the independent claims. Thus, a notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Applicant further notes that the prior art is deficient with respect to the dependent claims. Just by way of example, with respect to Claim 10 et al., the Examiner has relied on Col. 11, lines 8-15; and Col. 14, line 10-Col. 15, line 10 in Jenevein to make a prior

art showing of applicant's claimed technique "wherein validating the integrity of an object comprises determining that the object does not occupy a flagged inode and directory block." Applicant respectfully asserts that the excerpts relied on by the Examiner only relate to storage locations for images and an image locater. Clearly, determining a location of an image, as in Jenevein, does not even suggest "validating the integrity of an object," as specifically claimed by applicant (emphasis added).

With respect to Claim 12 et al., the Examiner has relied on Col. 2, lines 28-35 in Jenevein to make a prior art showing of applicant's claimed technique "wherein the real-time monitoring system is a VxD program." Specifically, the Examiner has stated that applicant's claimed VxD program is met by Jenevein's disclosure of an "IBM Compatible program." Applicant respectfully asserts that such excerpt does not disclose an IBM Compatible program, as the Examiner contends, but instead only discloses an IBM compatible partition table. Furthermore, applicant asserts that merely disclosing an IBM compatible partition table, as in Jenevein, does not meet any sort of "real-time monitoring system [that] is a VxD program," as specifically claimed by applicant (emphasis added).

With respect to Claim 13 et al., the Examiner has relied on Col. 2, lines 30-39 in Jenevein to make a prior art showing of applicant's claimed technique "wherein the real-time monitoring system is a UNIX daemon." Applicant respectfully asserts that Jenevein expressly discloses an IBM compatible partition table in order to distinguish a partition table that would be compatible with UNIX computer systems. Thus, since Jenevein teaches an IBM compatible partition table, Jenevein simply cannot meet applicant's claimed "real-time monitoring system [that] is a UNIX daemon."

Since the Hartley reference, when taken alone and in combination with Jenevein fails to meet all of applicant's claim limitations, as noted above, a notice of allowance or a proper prior art showing of all of the claim limitations, in the context of the remaining elements, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P352/00.145.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100